

August 5, 2022

Office of the Attorney General
Colorado Department of Law
Ralph L. Carr Judicial Building
1300 Broadway, 10th Floor
Denver, CO 80203

RE: Joint Ad Trade Letter – Informal Pre-Rulemaking Comment on Colorado Privacy Act Regulations

Dear Office of the Colorado Attorney General:

On behalf of the advertising industry, we provide input below to inform the drafting of regulations implementing the Colorado Privacy Act (“CPA”). We and the companies we represent, many of whom do substantial business in Colorado, strongly believe consumers deserve meaningful privacy protections supported by reasonable laws and responsible industry policies. We and our members therefore support a national standard for data privacy at the federal level, and, in line with this goal, we support harmonizing existing privacy standards in the states for the benefit of consumers and businesses alike.

As the nation’s leading advertising and marketing trade associations, we collectively represent thousands of companies across the country. These companies range from small businesses to household brands, long-standing and emerging publishers, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies that power the commercial Internet, which accounted for 12 percent of total U.S. gross domestic product (“GDP”) in 2020.¹ Our group has more than a decade’s worth of hands-on experience it can bring to bear on matters related to consumer privacy and controls. We welcome the opportunity to engage with you in this process to develop regulations to implement the CPA.

I. Colorado Should Take Steps to Harmonize Its Approach to Privacy with Other States When Such Harmonization Would Benefit Consumers and Controllers

In the absence of a national standard for data privacy at the federal level, it is critical for regulators to seriously consider the costs to both consumers and businesses that will accrue from a patchwork of differing privacy standards across the states. Harmonization with existing privacy laws is essential for creating an environment where consumers in Colorado and other states have a consistent set of expectations, while minimizing compliance costs for businesses. In line with the Colorado Attorney General’s (“CO AG”) goal of promoting “principle-guided rulemaking,” the regulations should “facilitate interoperability and help situate the CPA alongside the competing protections and obligations created by other state, national, and international frameworks” while also “not unduly burden[ing] anybody from developing creative, adaptive solutions to address challenges

¹ John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 15 (Oct. 18, 2021), located at https://www.iab.com/wp-content/uploads/2021/10/IAB_Economic_Impact_of_the_Market-Making_Internet_Study_2021-10.pdf (hereinafter, “Deighton & Kornfeld 2021”).

presented by advances in technology.”² In particular, Colorado has the opportunity to be a leader in the privacy space for the United States by implementing rules to effectuate key safeguards for universal opt-out mechanisms (“UOOMs”) that are explicitly referenced in the CPA itself, as well as providing flexibility for companies to communicate with and develop workable choice paths for consumers, as described in more detail below.

Compliance costs associated with divergent, and oftentimes conflicting, privacy laws are significant. To make the point: a regulatory impact assessment of the California Consumer Privacy Act of 2018 (“CCPA”) concluded that the initial compliance costs to California firms for the CCPA alone would be \$55 billion in just one state and without consideration for multi-state compliance.³ Additionally, a recent study on a proposed privacy bill in a different state found that the proposal would have generated a direct initial compliance cost of \$6.2 billion to \$21 billion, and an ongoing annual compliance cost of \$4.6 billion to \$12.7 billion for the state.⁴ Other studies confirm the staggering costs associated with varying state privacy standards. One report found that state privacy laws could impose out-of-state costs of between \$98 billion and \$112 billion annually, with costs exceeding \$1 trillion dollars over a 10-year period and small businesses shouldering a significant portion of the compliance cost burden.⁵ Colorado should not add to this compliance burden for businesses and should instead opt for an approach that is in harmony with existing state privacy laws if those state laws adopt standards that benefit all in the ecosystem.

II. The CPA Regulations Should Implement Key Statutory Safeguards Related to UOOMs

In the Colorado Attorney General’s pre-rulemaking considerations document, one area of particular emphasis for comments is UOOMs.⁶ The document specifically asks about key safeguards that are built into the text of the CPA to protect both consumers and businesses. These safeguards state that regulations defining technical specifications for UOOMs must:

- 1) Not permit the manufacturer of a platform, browser, device, or any other product offering a UOOM to “unfairly disadvantage another controller;”
- 2) Require controllers to “inform consumers about the opt-out choices available” (*i.e.*, the right to opt out of targeted advertising, sales of personal data, and profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer);

² Colorado Attorney General, *Pre-Rulemaking Considerations for the Colorado Privacy Act* at 2, located at <https://coag.gov/app/uploads/2022/04/Pre-Rulemaking-Considerations-for-the-Colorado-Privacy-Act.pdf> (hereinafter, “Pre-Rulemaking Document”).

³ See State of California Department of Justice Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations* at 11 (Aug. 2019), located at https://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

⁴ See Florida Tax Watch, *Who Knows What? An Independent Analysis of the Potential Effects of Consumer Data Privacy Legislation in Florida* at 2 (Oct. 2021), located at <https://floridatxwatch.org/DesktopModules/EasyDNNNews/DocumentDownload.ashx?portalid=210&moduleid=34407&articleid=19090&documentid=986>.

⁵ Daniel Castro, Luke Dascoli, and Gillian Diebold, *The Looming Cost of a Patchwork of State Privacy Laws* (Jan. 24, 2022), located at <https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws> (finding that small businesses would bear approximately \$20-23 billion of the out-of-state cost burden associated with state privacy law compliance annually).

⁶ Pre-Rulemaking Document at 2.

- 3) “Not adopt a mechanism that is a default setting, but rather clearly represents the consumer’s affirmative, freely given, and unambiguous choice to opt out of the processing of personal data” for purposes of targeted advertising or sales; and
- 4) Permit the controller to “accurately authenticate the consumer as a resident” of Colorado “and determine that the mechanism represents a legitimate request to opt out of the processing of personal data for purposes of targeted advertising or the sale of personal data.”⁷

We address each of these critical safeguards in turn below. UOOM regulations are one area where the CO AG can be a leader by setting standards that other states can look to for harmonization. Elaboration on and formal recognition of these safeguards in the CPA regulations is imperative to ensure Coloradans’ privacy choices are clearly described, effectuated uniformly throughout the marketplace, and tied to a clear consumer action showing an intent to make a specific choice.

a. UOOMs May Not Unfairly Disadvantage Controllers

The CPA explicitly prohibits creators of UOOMs from unfairly disadvantaging other controllers with their universal opt-out mechanism offerings. This safeguard is of key importance to prevent intermediary companies that stand between consumers and controllers online from developing UOOMs that unfairly restrict controllers from using personal data. For example, a mobile operating system should be prohibited from creating and offering a UOOM that broadcasts a user’s choice to opt out of targeted advertising or sales to all controllers in the online ecosystem while still using personal data for targeted advertising or sale purposes itself. For instance, if Apple were to implement a mechanism similar to its App Tracking & Transparency framework, it would unfairly disadvantage other controllers.⁸ Specifically, Apple’s App Tracking & Transparency framework provides a choice for consumers to universally “turn off tracking” by apps offered through the App Store, but the universal mechanism does not apply to Apple’s own use of personal data for targeted advertising and/or sales. The choice mechanism for Apple’s use of data for those purposes exists in a separate location, so users who employ the universal “tracking” control on iPhones are not making choices effective against Apple itself, the intermediary that stands between all companies who wish to engage with consumers via a mobile device. Intermediaries should not be permitted to offer UOOMs to the market in ways that entrench their position in the marketplace or make them subject to different standards or choice paths than other companies. The CO AG should issue regulations that clarify and ensure that companies offering UOOMs to the marketplace are subject to the very same limitations and opt out effects as other controllers against whom the UOOMs would be effective.

b. UOOMs Must Inform Consumers About the Opt Out Choices Available

The CPA states that the regulations must require controllers to inform consumers about the opt out choices available to them. The CO AG should issue regulations to clarify that entities who offer UOOMs to the marketplace must accurately describe the opt out choices available under Colorado law. Similarly, such UOOM creators should be required to ensure Coloradans are exposed to an explanation of the impacts of their privacy choices. For example, before an UOOM may be activated by a consumer, the regulations should require a disclosure that explains to consumer how their online experience may be impacted by virtue of their choice to enable the UOOM. Such a disclosure would help to provide the kind of “transparency [that] would meaningfully allow consumers to understand

⁷ Colo. Rev. Stat. § 6-1-1313(2)(f).

⁸ See Samuel Stolton, *Apple’s privacy rules targeted by German competition watchdog*, POLITICO EU (Jun. 14, 2022), located at <https://www.politico.eu/article/apples-privacy-rules-targeted-by-german-competition-watchdog/>.

the... processing of their personal data such that they can make informed opt out decisions.”⁹ As described in more detail in Section IV below, opting out of targeted advertising and/or sales across the entire online ecosystem through an UOOM is likely to impact a consumer’s digital experience. UOOM creators should be required to disclose factual information to consumers about the impacts of enabling an UOOM, and should be prohibited from editorializing or making normative statements about opt-out choices in ways that could induce a consumer to make a particular selection.

c. UOOMs Must Not Adopt a Default Setting Mechanism

The CPA clearly states that the UOOM regulations must prohibit default settings, and instead they must “clearly represent[] the consumer’s affirmative, freely given, and unambiguous choice to opt out of the processing of personal data.”¹⁰ This safeguard is intended to require a consumer to make a clear choice to opt out of the processing of personal data for purposes of targeted advertising or sales before the UOOM can be activated. Functionally, this requirement should be interpreted to mean that UOOM creators that turn such choice mechanisms on by default do not meet the CPA’s requirements for UOOMs to be clear representations of consumers’ affirmative choices.¹¹ The CO AG should promulgate rules that ensure a consumer must take an action to enable the UOOM before it can begin opting the consumer out of data transfers across the Internet.

In the CO AG’s pre-rulemaking considerations document, the CO AG asks whether “a tool that is marketed for its privacy features [would] suffice to satisfy [the] requirement” that UOOMs must be free from default settings.¹² Because the text of the CPA itself requires consumers to make an “affirmative, freely given, and unambiguous choice” to opt out, merely using a browser or a Bluetooth-enabled “smart product” like a lightbulb that automatically transmits a do not sell signal should not suffice to indicate a choice to turn on a UOOM. Allowing a consumer’s use of a marketed privacy feature to function as affirmative consent to opt out ignores the fact that the CPA permits consumers to opt out of multiple activities (targeted advertising and/or sales). Consumers consequently should have granular options to choose which activities they wish to opt out from. A tool that is marketed for its privacy features would inevitably make a choice for consumers without giving them the option to make particularized choices themselves. Tools and products are often bundled and marketed to consumers to feature numerous attributes, so attempts to discern which one of those attributes may or may not have spurred a consumer’s purchase, download, or use is an uncertain task. The reality is that consumers choose to use certain tools or products for multiple reasons, and assuming a consumer purchases, downloads, or uses a tool solely for its privacy features should not be a substitute for actual user-enabled consumer controls. The CO AG should include in its regulations text that clarifies UOOMs must obtain a consumer’s affirmative consent, via the clicking of a button or the checking of a box, and UOOM providers may not offer default settings that opt consumers out of activities automatically merely by virtue of being used, for example, on a consumer’s device.

d. UOOMs Must Permit a Controller to Accurately Authenticate the Consumer as a Colorado Resident

The CPA states that UOOMs must allow controllers to understand whether or not they are residents of Colorado. This requirement helps to ensure controllers will effectuate UOOM signals

⁹ Pre-Rulemaking Document at 5.

¹⁰ Colo. Rev. Stat. § 6-1-1313(2)(c).

¹¹ See Brave, *Global Privacy Control, a new Privacy Standard Proposal, now Available in Brave’s Desktop and Android Testing Versions*, located [here](#) (“Importantly, Brave does not require users to change anything to start using the GPC to assert your privacy rights. For versions of Brave that have GPC implemented, the feature is on by default and unconfigurable.”)

¹² Pre-Rulemaking Document at 3.

from Colorado residents consistent with the rights and obligations of the CPA. In the CO AG’s pre-rulemaking considerations document, the CO AG specifically asks what kind of mechanisms should the rules acknowledge to satisfy this requirement. The CO AG should issue regulations that require UOOMs to pass along a jurisdictional signal to controllers that indicates whether or not the consumer is a Colorado resident. Absent text in the regulations to clarify the requirement for UOOMs to disseminate a jurisdictional signal, controllers may not know whether a UOOM signal is coming from someone based in Colorado or in another location, where privacy rights and obligations may differ.

III. The CPA Dark Patterns Regulations Should Preserve Controllers’ Ability to Effectively and Flexibly Communicate with Consumers

The CO AG’s pre-rulemaking considerations document contemplates that the CO AG will issue rules to prohibit “dark patterns,” which the CPA defines to mean “a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice.”¹³ As the CO AG drafts regulations to guide such user interfaces, it should take steps to ensure controllers can convey critical information, rights, and choices to consumers in an effective and flexible fashion. For example, disclosures and choice paths that may be necessary for a controller that offers virtual reality experiences may be different than the disclosures and choice paths a controller that provides a mobile weather application must offer. Instead of requiring specific methods, modes, or content of communications between controllers and their customers to prevent dark patterns, we suggest that the CO AG promote options for flexibility in controllers’ communications with consumers.

Dark patterns regulations represent another area where the CO AG should take the lead to draft standards that protect consumers while enabling businesses to continue to communicate effectively with consumers. Overly simple, one-size-fits-all approaches like mandated symmetry in the number of steps to effectuate different choice patterns do not work for all companies that connect with consumers across various channels. For example, the user interface for a smart television may require more steps for users to make choices or use other mediums, like a web-based portal, to allow users to modify settings. The choice path for smart televisions therefore may reasonably differ from the choice path for a service that is available only via a web interface. Overly simplified regulations risk ignoring the reality that the path for exercising a privacy right may need to be different across channels, devices, and other modes of interaction between businesses and consumers. The CO AG should promote flexibility in its rules to ensure controllers of all types can comply with the regulations and effectively communicate with consumers.

IV. The Data-Driven and Ad-Supported Online Ecosystem Benefits Colorado Residents and Fuels Economic Growth

Over the past several decades, data-driven advertising has created a platform for innovation and tremendous growth opportunities. A recent study found that the Internet economy’s contribution to the United States’ GDP grew 22 percent per year since 2016, in a national economy that grows between two to three percent per year.¹⁴ In 2020 alone, it contributed \$2.45 trillion to the U.S.’s \$21.18 trillion GDP, which marks an eightfold growth from the Internet’s contribution to GDP in 2008 of \$300 billion.¹⁵ Additionally, more than 17 million jobs in the U.S. were generated by the commercial Internet in 2020, 7 million more than four years prior.¹⁶ More Internet jobs, 38 percent, were created by small firms and self-employed individuals than by the largest Internet companies, which generated

¹³ *Id.* at 4; Colo. Rev. Stat. § 6-1-1302(9).

¹⁴ Deighton & Kornfeld 2021 at 5.

¹⁵ *Id.*

¹⁶ *Id.*

34 percent.¹⁷ The same study found that the ad-supported Internet supported 154,403 full-time jobs across Colorado, more than double the number of Internet-driven jobs from 2016.¹⁸

A. Advertising Fuels Economic Growth

Data-driven advertising supports a competitive online marketplace and contributes to tremendous economic growth. Overly restrictive regulations that significantly hinders certain advertising practices, such as third-party tracking, could yield tens of billions of dollars in losses for the U.S. economy—and, importantly, not just in the advertising sector.¹⁹ One recent study found that “[t]he U.S. open web’s independent publishers and companies reliant on open web tech would lose between \$32 and \$39 billion in annual revenue by 2025” if third-party tracking were to end “without mitigation.”²⁰ That same study found that the lost revenue would become absorbed by “walled gardens,” or entrenched market players, thereby consolidating power and revenue in a small group of powerful entities.²¹ Smaller news and information publishers, multi-genre content publishers, and specialized research and user-generated content would lose more than an estimated \$15.5 billion in revenue.²² Data-driven advertising has thus helped to stratify economic market power and foster competition, ensuring that smaller online publishers can remain competitive with large global technology companies.

B. Advertising Supports Coloradans’ Access to Online Services and Content

In addition to providing economic benefits, data-driven advertising subsidizes the vast and varied free and low-cost content publishers offer consumers through the Internet, including public health announcements, news, and cutting-edge information. Advertising revenue is an important source of funds for digital publishers,²³ and decreased digital advertising budgets directly translate into lost profits for those outlets. Revenues from online advertising based on the responsible use of data support the cost of content that publishers provide and consumers value and expect.²⁴ And, consumers tell us that. In fact, consumer valued the benefit they receive from digital advertising-subsidized online content at \$1,404 per year in 2020—a 17% increase from 2016.²⁵ Regulatory frameworks that inhibit or restrict digital advertising can cripple news sites, blogs, online encyclopedias, and other vital

¹⁷ *Id.* at 6. See also Digital Advertising Alliance, *Summit Snapshot: Data Drives Small-and Mid-sized Business Online, It’s Imperative that Regulation not Short-Circuit Consumer Connections* (Aug. 17, 2021), located at <https://digitaladvertisingalliance.org/blog/summit-snapshot-data-drives-small-and-mid-sized-business-online-it%E2%80%99s-imperative-regulation-not>.

¹⁸ Compare Deighton & Kornfeld 2021. at 123 (Oct. 18, 2021), located [here](#) with John Deighton, Leora Kornfeld, and Marlon Gerra, *Economic Value of the Advertising-Supported Internet Ecosystem*, INTERACTIVE ADVERTISING BUREAU, 106 (2017), located [here](#) (finding that Internet employment contributed 67,895 full-time jobs to the Colorado workforce in 2016 and 154,403 jobs in 2020).

¹⁹ See John Deighton, *The Socioeconomic Impact of Internet Tracking* 4 (Feb. 2020), located at <https://www.iab.com/wp-content/uploads/2020/02/The-Socio-Economic-Impact-of-Internet-Tracking.pdf> (hereinafter, “Deighton 2020”)

²⁰ *Id.* at 34.

²¹ *Id.* at 15-16. See also Damien Geradin, Theano Karanikioti & Dimitrios Katsifis, *GDPR Myopia: how a well-intended regulation ended up favouring large online platforms - the case of ad tech*, EUROPEAN COMPETITION JOURNAL (Dec, 18, 2020), located at <https://www.tandfonline.com/doi/full/10.1080/17441056.2020.1848059>.

²² Deighton 2020 at 28.

²³ See Howard Beales, *The Value of Behavioral Targeting* 3 (2010), located at https://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

²⁴ See John Deighton & Peter A. Johnson, *The Value of Data: Consequences for Insight, Innovation & Efficiency in the US Economy* (2015), located at <https://www.ipc.be/~media/documents/public/markets/the-value-of-data-consequences-for-insight-innovation-and-efficiency-in-the-us-economy.pdf>.

²⁵ Digital Advertising Alliance, *Americans Value Free Ad-Supported Online Services at \$1,400/Year; Annual Value Jumps More Than \$200 Since 2016* (Sept. 28, 2020), located at <https://digitaladvertisingalliance.org/press-release/americans-value-free-ad-supported-online-services-1400year-annual-value-jumps-more-200>.

information repositories, and these unintended consequences also translate into a new tax on consumers. The effects of such regulatory frameworks ultimately harm consumers by reducing the availability of free or low-cost educational content that is available online.

C. Consumers Prefer Personalized Ads & Ad-Supported Digital Content and Media

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. One study found more than half of consumers (53 percent) desire relevant ads, and a significant majority (86 percent) desire tailored discounts for online products and services.²⁶ Additionally, in a recent Zogby survey conducted by the Digital Advertising Alliance, 90 percent of consumers stated that free content was important to the overall value of the Internet and 85 percent surveyed stated they prefer the existing ad-supported model, where most content is free, rather than a non-ad supported Internet where consumers must pay for most content.²⁷ Indeed, as the Federal Trade Commission noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.²⁸

During challenging societal and economic times such as those we are currently experiencing, laws that restrict access to information and economic growth can have lasting and damaging effects. The ability of consumers to provide, and companies to responsibly collect and use, consumer data has been an integral part of the dissemination of information and the fabric of our economy for decades. The collection and use of data are vital to our daily lives, as much of the content we consume over the Internet is powered by open flows of information that are supported by advertising. We therefore respectfully ask you to carefully consider any future rule's potential impact on advertising, the consumers who reap the benefits of such advertising, and the overall economy before advancing it through the regulatory process.

* * *

²⁶ Mark Sableman, Heather Shoenberger & Esther Thorson, *Consumer Attitudes Toward Relevant Online Behavioral Advertising: Crucial Evidence in the Data Privacy Debates* (2013), located at https://www.thompsoncoburn.com/docs/default-source/Blog-documents/consumer-attitudes-toward-relevant-online-behavioral-advertising-crucial-evidence-in-the-data-privacy-debates.pdf?sfvrsn=86d44cea_0.

²⁷ Digital Advertising Alliance, *Zogby Analytics Public Opinion Survey on Value of the Ad-Supported Internet Summary Report* (May 2016), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/ZogbyAnalyticsConsumerValueStudy2016.pdf.

²⁸ Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018), located at https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.

We and our members support protecting consumer privacy. We thank you for considering our comments above on the need for harmonization across state privacy standards, the importance of key safeguards for UOOMs that are enshrined the CPA itself, and the need for flexibility in any regulations the CO AG may promulgate regarding dark patterns. We look forward to continuing to work with you as your office releases proposed regulations to implement the CPA.

Thank you in advance for consideration of this letter.

Sincerely,

Christopher Oswald
EVP, Government Relations
Association of National Advertisers
202-269-1883

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's
202-355-4564

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
703-220-5943

Lartase Tiffith
Executive Vice President for Public Policy
Interactive Advertising Bureau
212-380-4700

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
202-898-0089

Lou Mastria, CIPP, CISSP
Executive Director
Digital Advertising Alliance
347-770-0322

CC: Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP